

**Office of the
Attorney General**

A Parents' Guide to Social Networking Websites



FEBRUARY 2010

LAWRENCE WASDEN
Attorney General
700 West Jefferson Street
Boise, ID 83720-0010
www.ag.idaho.gov

20 Internet Acronyms Every Parent Should Know

1. A/S/L.....Age/sex/location
2. DOC.....Drug of choice
3. GYPO.....Get your pants off
4. ITSIntense text sex
5. IWSNI want sex now
6. KPC.....Keeping parents clueless
7. LHSOLet's have sex online
8. LMIRLLet's meet in real life
9. NIFOCNude in front of computer
10. P911Parent alert
11. PAW.....Parents are watching
12. PIRParent in room
13. POSParent over shoulder
14. PRON.....Porn(ography)
15. RUO18.....Are you over 18?
16. SorG.....Straight or gay
17. TDTMTalk dirty to me
18. WUF.....Where are you from?
19. WYCM.....Will you call me
20. WYRNWhat's your real name?



State of Idaho Office of Attorney General Lawrence Wasden

Dear Parents:

We teach our children not to talk to strangers. We instill in them the importance of never opening the door for someone they do not recognize, never getting into an unfamiliar car, and never being out alone when it's dark.

Prior to the Internet explosion, these precautions seemed adequate. In today's world, however, children are exposed to strangers posting sexually explicit images or looking for sex on the Internet. Internet predators can contact children in their homes at any time of the day or night via social networking sites, e-mail, instant messages and chat rooms.

Social networking websites are very popular with people of all ages, but they especially draw the attention of young adults. These websites have names such as Facebook.com, MySpace.com, and YouTube.com. Individuals access these sites to chat with friends and family, meet new people, share photos and videos, and to post online journals (more commonly known as blogs) about their lives.

Teens use these websites to socialize online with friends. They often express themselves by posting stories, feelings, photos, and videos. Unfortunately, sexual predators also use these websites to meet and groom potential victims, including teens. Young adults also run the risk of being exposed to sexual images and materials, or becoming the victim of online harassment by their peers, also known as

cyberbullying.

To better protect your children, I encourage you to learn more about social networking websites and how they work. My office has prepared this guide to help close the technology gap between parents and teens.

After reading this guide, you may want to view the ProtecTeens™ video for more information about online safety. The ProtecTeens resource kit contains a Family Internet Contract, Internet Safety Manual, Internet Lingo Dictionary and Parental Control Information guide (which discusses computer and software settings). You can view the ProtecTeens video and these materials, or request copies by mail, by visiting www.ag.idaho.gov.

LAWRENCE G. WASDEN
Attorney General

Table of Contents

WHAT IS ONLINE SOCIAL NETWORKING?	1
WHAT IS AN ONLINE PROFILE?	3
CREATING A PROFILE	8
HOW CAN I FIND OUT IF MY CHILD HAS A PROFILE?	10
WHAT ARE “FRIENDS”?	11
SECURITY AND PRIVACY SETTINGS	13
FACEBOOK	15
MYSPACE.....	19
INFORMATION POSTED IN A PROFILE	22
PERSONAL INFORMATION.....	22
PHOTOS AND VIDEOS	23
COMMUNICATIONS.....	25
<i>Comments and Wall Posts.....</i>	<i>25</i>
<i>News Feeds and Streams.....</i>	<i>28</i>
<i>Instant Messaging</i>	<i>31</i>
<i>Applications</i>	<i>33</i>
<i>Blogs.....</i>	<i>35</i>
<i>Mail Messages.....</i>	<i>35</i>
<i>Chat Rooms</i>	<i>36</i>
WHAT I CAN DO TO KEEP MY CHILD SAFE	38
UNDERSTAND CYBERBULLYING.....	40
<i>Forms of Cyberbullying</i>	<i>40</i>
<i>Victims of Cyberbullying.....</i>	<i>41</i>
DELETING A PROFILE	42

WHAT IS ONLINE SOCIAL NETWORKING?

A social networking website is a virtual community where people create “profiles” to post pictures, videos, blogs, and information about themselves to share with friends and family. Some of the more popular social networking websites are Facebook.com, MySpace.com, YouTube.com, myYearbook.com, Twitter.com, and Mocospace.com.

Anyone with access to the Internet can create a profile. Once a profile is created, that person, or “member,” can link their profile to other people, or “friends.” Once linked, members can view and contribute to each others’ profiles.

The most popular things to share online with friends are pictures, videos, “blogs,” and comments or “wall posts.” However, kids also post information such as phone numbers, what school they attend, and even their address. This can create an opportunity for strangers to gain access to a child.

Social networking is growing at an astonishing rate. NetSmartz.org has reported that 61% of 13-to-17-year-olds have posted a personal profile on a social networking website, and that 50% of them have posted photos of themselves online. According to a separate report entitled *How Teens Use Media*, prepared by the Nielsen Company in 2009, 90% of teens have access to the Internet in their homes, and 73% have access at their school. Teenagers in the United States spend an estimated average of 11 hours and 32 minutes each month using the Internet.

In December 2009, Facebook.com, MySpace.com and YouTube.com were ranked as the three most visited social networking websites. Facebook reportedly has more than 350 million active users worldwide. MySpace is a close second, with 269 million. According to the Nielsen report,

67% of teens that have profiles on social networking sites update those profiles at least once a week.

Gaming websites and online gaming services, available through consoles, such as Nintendo Wii, PlayStation, and Xbox, are another form of social networking. Players can create profiles and chat with other players. They can even interact with other players in real-time by using headsets and webcams to speak to and see other players. Some examples of popular games among young people are World of Warcraft, Halo, Second Life, Call of Duty, and Gears of War.

With all of the latest statistics, it is obvious that our children are becoming more and more aware of social networking websites. Unfortunately, sexual predators can also use these websites to meet and victimize children. Predators frequently pose as a sympathetic adult who “really understands” a teen’s problems. These predators often devote a considerable amount of time to grooming their victims with attention and friendliness. The predator’s ultimate goal is meeting the child in person for sex.

In August 2006, the National Center for Missing & Exploited Children and co-sponsors published *Online Victimization of Youth: Five Years Later*, which reports the results of a nationwide survey of 1,500 children, ages 10 to 17. The 2006 report identifies safety risks to children using the Internet and highlights the following findings:

- 34% (1 in 3) of the children surveyed saw unwanted sexual material online, despite increased use of filtering, blocking and monitoring software.
- 9% (1 in 11) of the children surveyed encountered harassment online, including rude, hostile and aggressive behaviors.

- 13% (1 in 7) of the children surveyed received unwanted sexual solicitations online (not only from strangers but also from their peers). 4% of the children surveyed received aggressive sexual solicitations (where a solicitor asked to meet in person, called on the telephone, or sent money, mail or gifts).


Given the popularity of social networking websites, it is very important that parents of teens learn how to use them.

WHAT IS AN ONLINE PROFILE?

A “profile” is a collection of personal information created by an individual that is shared among online friends. A basic profile can contain as little as an individual’s name, age, and sex. However, most profiles include much more information about an individual. Teens often post nicknames, e-mail addresses, phone numbers, hometown location, birth date, photos, videos, clubs they belong to, hobbies they have, schools they attend, movies and books they like, music they listen to, places they work, and sports teams they are part of. Profiles can also be linked to blogs, bulletin boards, e-mail, chat rooms, and calendars.

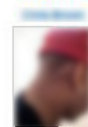
Profiles offer teens an excellent source of self expression. They often decorate their profiles with special backgrounds and fonts, animations, photos, music, and videos that describe them. A lot of effort goes into these visual effects. However, teens may think they are posting information that will only be shared with their friends. They fail to realize that their online profiles could be seen by potential employers or college admissions counselors. They may also be unaware that the information in their profiles can create a trail of clues for sexual predators.

Knowing what types of information your child is posting is the first step in keeping them safe online. To see what teens post on profiles, get online and look at some profiles. The following are examples from three popular social networking websites.

Hayden
15 / Female
BOISE, US
Last Login: 11/16/2009
 Online Now!

Add Comment

Occupation: Student




MEZ_HOOZTIN



Heveson







Sign Out

[Home](#)
[Videos](#)
[Channels](#)
[Shows](#)

[Subscriptions](#)
[History](#)


[Subscribe](#)
All
Uploads
Favorites
Playlists
1 P
≡



0:43 / 3:12
HQ

Info
Comments
Favorite
Share
Playlists
Flag

cat


From: [redacted] | January 2, 2010 | 24 views

lolz :3 shes so cute


1 ratings ★★★★★

[View comments, related videos, and more](#)


Uploads (10)



cat
18 views - 2 months ago




Out of control
19 views - 2 months ago




Not Good Enough
16 views - 2 months ago

[see all](#)


Favorites (445)



revolution by the beatles lyrics
views - 213,941




Flyleaf - Sorrow
views - 3,244,193



Hellsing- Phantom of the Opera
- 1,356 views

[see all](#)



[Subscribe](#)

[Add as Friend](#) | [Block User](#) | [Send Message](#)

Profile

Name: Haylee

Channel Views: 580

Age: 15

Joined: August 15, 2008

Last Sign In: 4 days ago




Subscribers: 4




Hometown: Lewiston, Idaho

Country: United States

[Report profile image violation](#)


Subscriptions (7)






[see all](#)


Recent Activity




rated a video: ★★★★★ (2 months ago)




After seeing Miyavi's Itoshii Hito music video I instantly loved it so I decided to take one of his live performances (At the beautiful's fest '03... [more](#)




favorited a video (2 months ago)




Flyleaf - Sorrow
Music video by Flyleaf performing Sorrow with Jake Davis [Video Director], Kerri Kleiner [Video Producer] (C) 2008 OctoScope Music, LLC



became friends with [redacted] (5 months ago)







became friends with [redacted] (5 months ago)










became friends with [redacted] (5 months ago)

Subscribers (4)







Friends (21)

[see all](#)

Channel Comments (9)



(4 months ago)

hola!! tiz Haru-Koh!! i watched ur videos! they tiz amazing!! X3

[Spam](#)

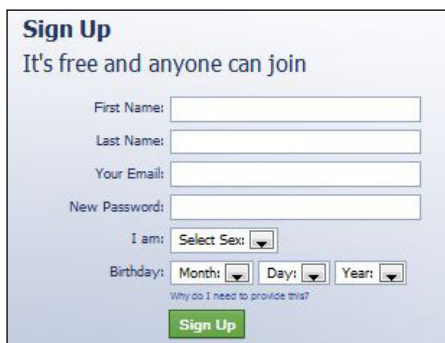
CREATING A PROFILE

It is very easy to create a profile. You can do it in under 60 seconds with just a few short steps. Any teen or younger child with intermediate Internet knowledge can set up a profile on a social networking website, even without your knowledge or consent.

You need only minimal information to set up a profile, usually only a first and last name, date of birth, and an e-mail address. You always need an e-mail address to set up a profile. Similarly, kids can set up an e-mail address with minimal Internet knowledge and without parental consent. There are many popular e-mail services available, such as Yahoo, HotMail, and Gmail.

Some, **but not all**, social networking websites and e-mail services impose a minimum age restriction of 13 years old for new members. However, children under the age of 13 can easily gain access by lying about the year they were born to make them appear older.

The following examples give you an idea of how little information is needed for your child to set up a social networking account.



The image shows a screenshot of the Facebook 'Sign Up' form. At the top, it says 'Sign Up' in bold blue text, followed by 'It's free and anyone can join' in a smaller blue font. Below this are five input fields: 'First Name:', 'Last Name:', 'Your Email:', and 'New Password:'. Under the 'New Password:' field is a dropdown menu labeled 'I am: Select Sex:'. Below that is a 'Birthday:' section with three dropdown menus for 'Month:', 'Day:', and 'Year:'. A small blue link 'Why do I need to provide this?' is located below the birthday fields. At the bottom of the form is a green button with the text 'Sign Up' in white.

Facebook

Sign Up for MySpace

Email Address:

Password:

Full Name:

Date Of Birth: Month Day Year

Gender: ☐ Female ☐ Male

Sign Up

MySpace

User Name:

Password:

Email Address:

Date of Birth: Month Day Year

Gender: ☒ Female ☐ Male

Area Code:



Enter the text from the image:

Sign Up

MocoSpace

Full name


Username

Your URL: <http://twitter.com/USERNAME>

Password

Email

☒ I want the inside scoop—please send me email updates!



Type the words above

Can't read this?
[Get two new words](#)
[Hear a set of words](#)
 Powered by [reCAPTCHA](#)
[help](#)

Create my account

Twitter

HOW CAN I FIND OUT IF MY CHILD HAS A PROFILE?

Start by asking your child. Your child may have profiles on more than one website.

Most social networking websites have a search function to help people find people. Use this feature to find out if your child has a profile. Searching for your child's e-mail address on a social networking website is the fastest and most accurate way to find your child's profile. If you do not know your child's e-mail address, search for your child's name.

Common names often return hundreds, if not thousands, of search hits. On most sites, you can narrow your search by using the location, age, and gender filtering options.

If you suspect that your child has a profile on a social networking website but cannot locate it, try searching the website for your child's friends. If you find a public profile for one of your child's friends, navigate through his or her friends list to see if your child is a member of the network.

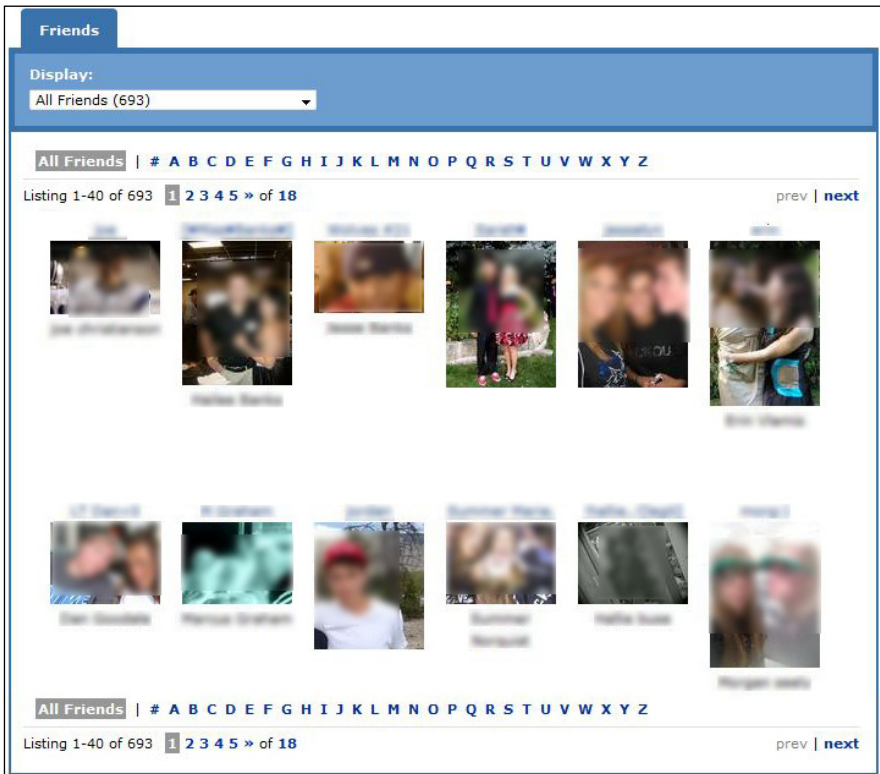
You can also try to do a general search from the search toolbar. Try different search options, such as your child's cell phone number, sports teams, or nickname.

On your home computers, you can search the Internet history from your Internet browser to check what sites have been visited. There are many different browsers available. Three popular browsers are Internet Explorer, Safari, and Firefox. As you browse, look for website addresses of social networking sites, such as Facebook.com, MySpace.com, MocoSpace.Com, YouTube.com, myYearbook.com, and Twitter.com.

WHAT ARE “FRIENDS”?

Members of social networking websites who link their profiles with other profiles are called “friends.” Members can expand their list of “friends” by requesting that other members add them as a “friend,” or by accepting invitations from other members to be added to their “friends” lists.

The following image is an example of a “friends” list.

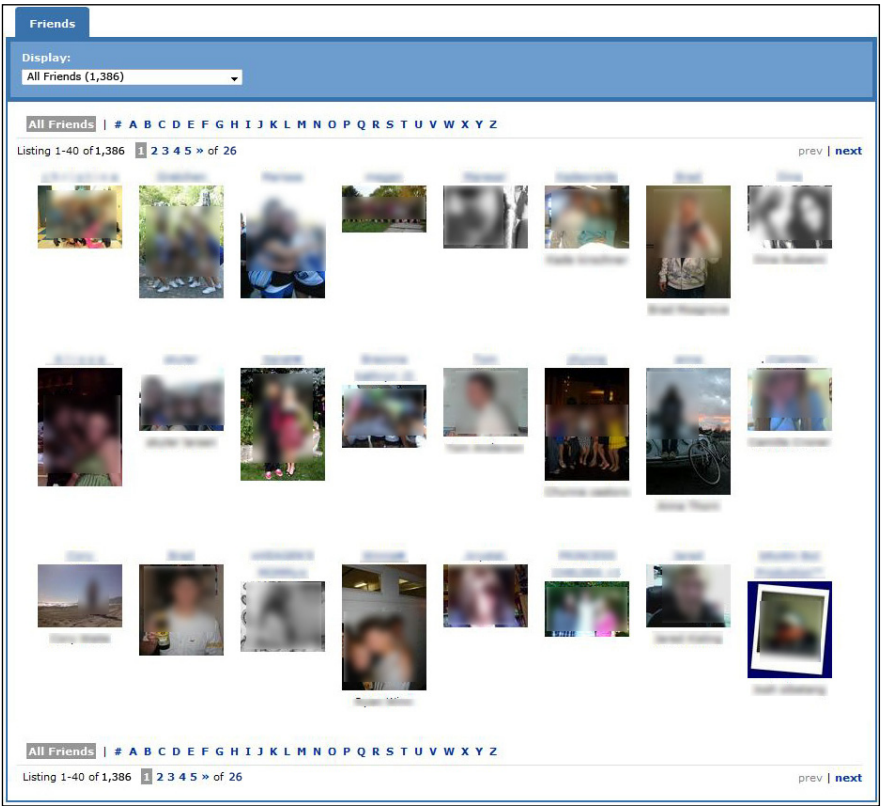


MySpace Friend List

Adding friends is the backbone to social networking, and it appeals to teens who want to spend time online with friends. Unfortunately, teens also use these “friends” lists to fuel popularity contests. The larger the list of friends, the more

popular a teen appears to be. This is known as “micro-celebrity,” and can lead teens to add people as a “friend” that they don’t know in the real world.

In the following example, a 17-year-old girl has a list of 1,386 “friends” in MySpace. This gives all 1,386 people access to her personal information. More than likely, this 17-year-old does not really have over 1,300 friends. It is possible that one or more of these friends is a sexual predator.



MySpace Friend List

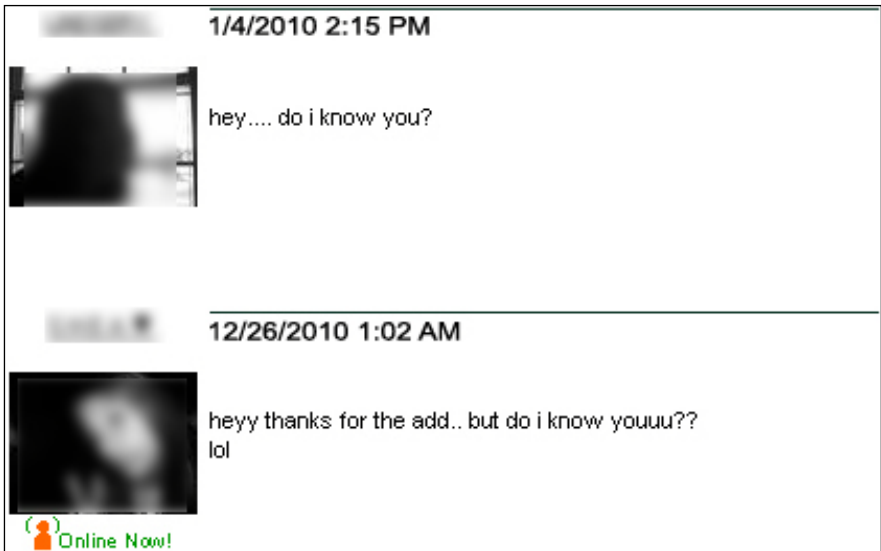
Predators often disguise themselves by setting up false profiles and pretending to be a young girl or boy just to meet

kids online. If a child accepts a “friend request” from a predator, it allows that predator to see everything on the child’s profile page. Once they are “friends,” having their profile set to “private” will not matter. The predator will be able to see anything on that child’s profile, including photos and the child’s friend list, even contact and location information. Your children need to be very cautious of who they add to their “friend” lists.

SECURITY AND PRIVACY SETTINGS

By default, anyone can see a profile that is newly added. (Some social networking websites may automatically adjust this setting if the new user’s date of birth is set to under the age of 18.) Photographs, videos, blogs, comments, pictures of friends, wall posts, and comments on the profile can be viewed by anyone—friend or stranger. Therefore, it is very important that you and your child know how to set the profile privacy options on all of your child’s social networking accounts.

However, setting privacy options is no guarantee of safety. Teens can still add strangers to their “friends” lists, giving those strangers access to personal information. The danger is that these unknown “friends” could be sexual predators. The following example shows two separate “friends” who accepted a “friend” request from a person they don’t know.



MySpace

Social networking websites rely on users to be truthful, but there is nothing to prevent a predator from lying about his or her age in order to appear to be a teen. A 40-year-old predator could easily create a profile claiming to be 17. This person would then have full access to the “private” profile of anyone who unknowingly designated the predator as a friend. It is important to teach your teen to only add people they know in real life as friends.

Social networking websites all have very similar security settings. There are literally hundreds of combinations for those settings. How a member designates those combinations will determine how a profile will be viewed by others. You should make yourself familiar with all security settings and set up the proper options with your teen to help protect them against strangers on the Internet.

Because there are so many different combinations of security settings, the following examples are meant only to be used as a guide for showing you where the options are located within

the most popular social networking websites. These examples are not intended to give you direction on which privacy options you should set. You can better determine which security options should be in place for your child.

FACEBOOK

Information such as name, hometown, relationship status, schools, education, and e-mail address can be found by clicking on the “Profile” option from the toolbar...



...then selecting the “Info” tab next to the “Wall.” The “Edit” tool can be used to modify each section.

A screenshot of a Facebook profile's 'Info' page. At the top, there are tabs for 'Wall', 'Info', and a '+' icon. To the right of the 'Info' tab is a link that says 'Edit Information' with a pencil icon. The page is divided into several sections: 'Basic Information', 'Contact Information', and 'Education and Work'. Each section contains various fields and their corresponding values, with an 'Edit' button (pencil icon) next to each field.

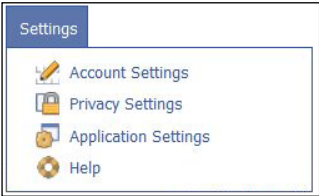
Basic Information	
Sex:	Female
Birthday:	June 2, 1995
Hometown:	Southeast Boise, Boise, ID
Relationship Status:	In an Open Relationship
Looking For:	Friendship Dating A Relationship
Religious Views:	Christian - Catholic

Contact Information	
Email:	qtcupcake@live.com
Mobile Number:	208-555-7431
Other:	208-555-6037
Current Address:	555 Main Street Southeast Boise, Boise, ID 83706
Google Talk:	qtcupcake
AIM:	qtpiecupcake
Windows Live:	qtpiecupcake

Education and Work	
High School:	Timberline High School
Employer:	Starbucks
Location:	Boise, ID

Facebook “Info” Page

The general privacy settings for a Facebook member can be located under the “Settings” portion of the member’s webpage. Security is broken down into three sections: Account Settings, Privacy Settings, and Application Settings. These options are found under “Settings” from the top toolbar:



Facebook Settings

The “Account Settings” contains items such as name, e-mail address, password, and mobile options for cell phone activation. This is also where the option to deactivate the profile is located.

Settings	Networks	Notifications	Mobile	Language	Payments	Facebook Ads
Name change						
Your real name. Hayden Messenger						
Username change						
Your username						
Email change						
Set your email contact information. qtcupcake@live.com						
Password change						
What you use to log in. *****						
Linked Accounts change						
Use other accounts to log in.						
Security Question change						
To identify you as the account owner.						
Privacy manage						
Control what information you share.						
Deactivate Account deactivate						

Facebook Account Settings

“Privacy Settings” allow you to control who is allowed to view the profile and its contents. There are settings for the profile page, searching visibility, news feed and status activity, wall post visibility, and application control. This is also where the Facebook block list is located.

Privacy Settings



Profile Information

Control who can see your profile and who can post to your Wall



Contact Information

Control who can contact you on Facebook and see your contact information and email



Applications and Websites

Control what information is available to Facebook-enhanced applications and websites



Search

Control who can see your search result on Facebook and in search engines

















Block List

Control who can interact with you on Facebook

Facebook Privacy Settings

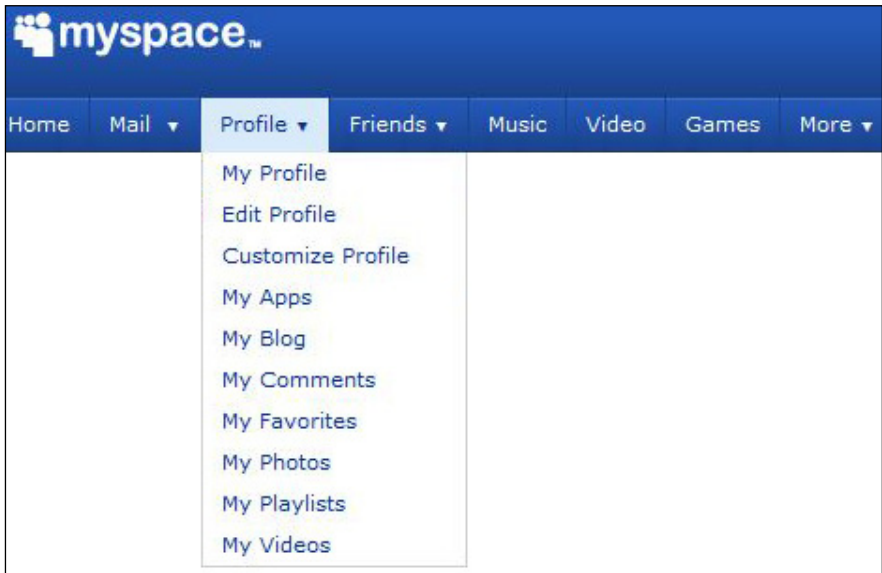
“Application Settings” details which applications the profile has authorized to use and what permissions are granted to those applications.

Application Settings - Granted Additional Permissions			
Displaying 42 applications you have granted additional permissions.		Show:	Granted Additional Permissions ▾
▼ Publish recent activity (one line stories) to my Wall			
 Bumper Sticker	Edit Settings	Profile	X
 Daily Friends	Edit Settings	Profile	X
 Date of the Day	Edit Settings	Profile	X
 Events	Edit Settings	Profile	X
 FarmVille	Edit Settings	Profile	X
 Gifts	Edit Settings	Profile	X
 Groups	Edit Settings	Profile	X
 Links	Edit Settings	Profile	X
 Notes	Edit Settings	Profile	X
 Photos	Edit Settings	Profile	X
 Pieces of Flair	Edit Settings	Profile	X
 Quizzaz	Edit Settings	Profile	X
 Sketch Me	Edit Settings	Profile	X
 The Mood Weather Report	Edit Settings	Profile	X

Facebook Application Settings

MYSPACE

You access profile information by selecting “Edit Profile” from the “Profile” option on the toolbar.




All general information, such as name, school, interests, location, hometown, etc., can be accessed and modified using the menu in the left margin:

About Me Interests Basic Info Details Schools Companies Networking	Contact Information
	Display Name: <input type="text" value="Hayden"/>
	First Name: <input type="text" value="Hayden"/>
	Last Name: <input type="text" value="Messenger"/>
	Basic Info
	Headline: <input type="text"/>
	Gender: <input type="radio"/> Male <input checked="" type="radio"/> Female
	Date Of Birth: <input type="text" value="Jun"/> / <input type="text" value="2"/> / <input type="text" value="1995"/>
	City: <input type="text" value="Boise"/>
	Country: <input type="text" value="United States"/>
Region: <input type="text" value="Idaho"/>	
Zip Code: <input type="text" value="83706"/>	

MySpace Profile Editing

The “Account Settings” option contains the security and privacy settings. There are many other options in this area, including e-mail address, and settings for password, spam, Instant Message (IM), Applications, and mobile phone activation. The option to cancel a MySpace account is also located here, under the “Account Cancellation” selection.

 **account settings** [View My Profile](#) [Edit Profile](#) [Customize Profile](#)

[Contact Info](#) | [Account](#) | [Password](#) | [Privacy](#) | [Spam](#) | [Notifications](#) | [Applications](#) | [IM](#) | [Mobile](#) | [Calendar](#) | [Miscellaneous](#)
[Ad Categories](#) | [No More CAPTCHAs](#) | [Sync](#)

Email Address

Contact Address :

Account Settings

Preferred Site & Language :

Time Zone : (GMT -7 hour)

Time Zone: To make it easier on our users we synched your MySpace time zone to your computer clock. If you need to update your MySpace time, change the time of your computer to update.

Account Cancellation

Account Cancellation : [Cancel Account](#)

Contact Address: MySpace uses your email address to send you important information, such as login information and change verifications, as well as notifications you set in the Notifications Settings. We do not spam.

Preferred Site & Language: Changing your preferred site doesn't change your friends or how you meet people.

MySpace Account Settings and Privacy Options

INFORMATION POSTED IN A PROFILE

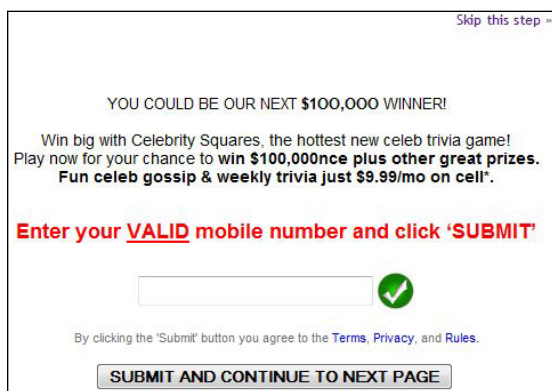
PERSONAL INFORMATION

Teens unwittingly post a wide range of personal information on their profiles. Social networking websites encourage new members to supply personal data, such as their relationship status, sexual orientation, religion, body type, and ethnicity. Teens also add their personal interests, such as what books they read, what movies they watch, and what music they listen to. These details are displayed in the member's profile:

Interests
General
Volleyball, friends, cell phone, and THE MALL!!!! Shopping is our friend ;)
Music
I love all kinds of music... Lady Gaga, Beyonce, Lil Wayne, Jay-Z, Kanya West, Kings of Leon, Chris Brown, Black Eyed Peas, Britney Spears, Owl City, Jack Johnson, AC/DC, Metalica, Dave Matthews, Mickey Avalon, Lil Jon, Kid Rock, Flo Rida, T-Pain, Savage.... the list goes on and on and on...
Movies
Of course... Twilight and New Moon, Paranormal Activity, The Blind Side, Lovely Bones, and Avatar . I also loved Love old ones too like Titanic, Princess Bride, ET, Dirty Dancing... and my favorite... The Breakfast Club.
Books
All of the Twilight books!
Details
Status: Single
Here for: Networking, Dating, Friends
Hometown: Boise
Orientation: Straight
Body type: 5' 2" / Athletic
Ethnicity: White / Caucasian
Religion: Catholic
Zodiac Sign: Libra
Children: Someday
Occupation: Timberline High School 2013

MySpace

Social networking websites often display automatically generated questions for members to answer concerning their personal information. Some websites go as far as asking for your child's cell phone number. The following is an example from MocoSpace, asking a new member for their cell phone number:

A screenshot of a MocoSpace registration form. At the top right, there is a link that says "Skip this step >". The main text in the center reads: "YOU COULD BE OUR NEXT \$100,000 WINNER! Win big with Celebrity Squares, the hottest new celeb trivia game! Play now for your chance to win \$100,000 once plus other great prizes. Fun celeb gossip & weekly trivia just \$9.99/mo on cell!". Below this, in red text, it says "Enter your VALID mobile number and click 'SUBMIT'". There is a text input field for the mobile number, followed by a green circular icon with a white checkmark. Below the input field, it says "By clicking the 'Submit' button you agree to the [Terms](#), [Privacy](#), and [Rules](#)." At the bottom, there is a button that says "SUBMIT AND CONTINUE TO NEXT PAGE".

MocoSpace

Although there is an option to “skip this step,” you can see that the invitation to enter a cell phone number is much more prominent.

PHOTOS AND VIDEOS

Social networking websites encourage members to upload photos and videos of themselves to their profiles for others to view. This is a large part of why teens like social networking. It allows them to share their digital memories with friends. However, most default securities allow anyone to see the pictures and videos.

Other members can also leave comments on your teen's photos and videos. By default, most profile securities allow anyone to add comments. This can be very damaging if the comments are mean or derogatory. The following is an example of a photo with comments left by other members.

the photo, and then that photo will also show up on your child's profile pictures. If tagging securities are not properly set, anyone can see these photos.

COMMUNICATIONS

Social networking websites offer many different ways for friends to communicate with one another, such as News Feeds, Streams, Wall Posts, Bulletin Space, and Comments. They may have different names, but they are all very similar. Teens use these tools to communicate back and forth with their friends.





Teens often use abbreviations and acronyms when posting communications and conversations online. This type of short form writing is called Internet "lingo." A list of the Top 20 Internet Acronyms is provided at the front of this guide. The *Internet Lingo Dictionary*, which is available on the ProtecTeens DVD and at www.ag.idaho.gov, provides a more extensive list.

Comments and Wall Posts

Members can add content to another member's page by using the "Wall" and "Comments" features. These types of web posts are conversations between two or more people. The comments posted to someone's Wall or Comment area can be seen by anyone with access to that profile.

To view “Comments” on a MySpace profile, scroll down the profile page until you find the comments area.

displaying 25 of 2289 comments ([view all](#) | [add comment](#))

 Emily Howard	Jan 12, 2010 11:30 PM Hahah that's cute :) Yeah I was planning on coming home and going to sleep all day and then i went to sleep in class for an hour and a half so i'm not really all that tired anymore haha
 [Name obscured]	Jan 12, 2010 10:28 PM boyfriend lied to me last nite. and now idk wat to even say to him. cuz im so hurt
 [Name obscured]	Jan 12, 2010 10:20 PM whats goin on with you tonight girl. :)
 [Name obscured]	Jan 12, 2010 10:02 PM hey cutie wats been up

Myspace Comments

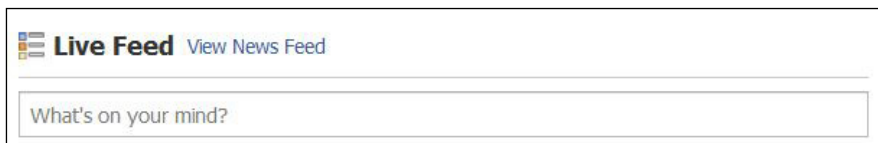
To view someone’s “Wall” in Facebook, go to that person’s profile and select the “Wall” tab.



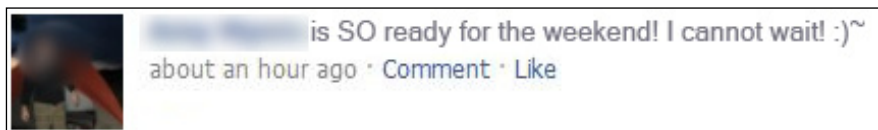
Facebook Wall

News Feeds and Streams

Real-time updates to profiles belonging to people on your teen's friend list can be seen on Facebook's News Feed (or Live Feed) and on Myspace's Streams. When users post to these areas, it comes across as a mass message to all mutual friends. For example, on Facebook, if a user posts something to the area "What's on your mind?"...



...it will be displayed on their News Feed, as well as their friends':



"Status" and "Activity" updates also show up as News Feeds and Streams. These forms of updates encompass many things, such as a change in mood, relationship status, change of e-mail address, or when someone adds a new friend.

The following are examples from two popular social networking websites.

 **Live Feed** [View News Feed](#)

What's on your mind?



[Jeff Williams](#) and [Jennifer Rose \(Hend\)](#) are now friends.
 2 hours ago · [Comment](#) · [Like](#)



[Ashley Waples](#) went from being "in a relationship" to "single."
 12 hours ago · [Comment](#) · [Like](#)




[Amy Wynn](#) and [Curtis Prescott](#) are now friends.
 Yesterday at 9:51pm




[Ashley Waples](#) became a fan of [I have no idea what you just said so im just gonna say "yeah" and smile.](#)
 Tue at 8:03pm · [Comment](#) · [Like](#) · [Become a Fan](#)

Facebook Status Activity on News Feed

 **Stream**

view all: [status & mood](#) | [activities](#)




shes here :)

Mood: happy 🍷🍷

Posted 5 hours ago

[view more](#) | [comment](#)




is chill

Mood: chill 😊

Posted 17 hours ago

[view more](#) | [comment](#)




going dumb

Mood: super duper supe 😊

Posted 17 hours ago

[view more](#) | [comment](#)




Bored help me

Mood: 208-890-9694

Posted 19 hours ago

[view more](#) | [comment](#)



set up a new email address:
@myspace.com.
Get your own @myspace.com email address!

Posted at 2:54 PM Nov 17

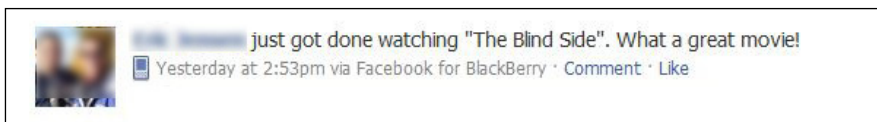
view all: [status & mood](#) | [activities](#)

Myspace Status Activity on Stream

It is also important to know that many, many teens are now using the mobile side of social networking from their cell phones. Originally, Twitter was most commonly known for this service. However, MySpace and Facebook have jumped

onboard the mobile wagon. Teens can access their social networking sites from their cell phone, even if the cell phone service does not include Internet service. Anyone that has a cell phone with SMS (short for Short Message Service, better known as texting) can receive friend requests, messages, wall and comment posts, and status updates right to their phone. They can also update their own status, add pictures, and add news feeds.

The following are two examples of mobile posts from popular social networking websites.



Facebook Post from Mobile Device



MySpace Post from Mobile Device

Instant Messaging

Another draw for teens who use social networking websites is the ability to send instant messages, or chats, to their friends. Instant messaging allows friends to communicate one-on-one with each other instantly. It's like having a telephone conversation via the keyboard.

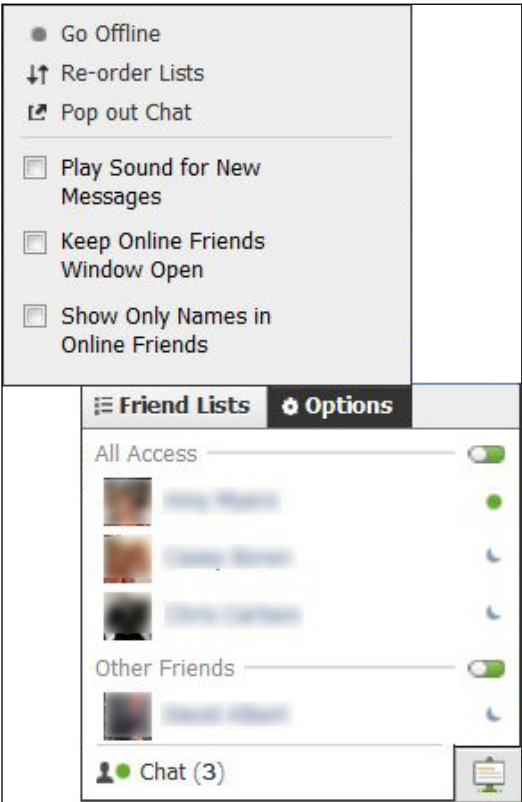
Instant messaging is available on both Facebook and MySpace. Both have basically the same look and feel. The following are examples from Facebook.

Facebook’s versions of instant messages are called “chats.” The chat display is at the bottom right corner of the Facebook window. It indicates how many people from a friend list are actively online. Here you can see that there are three friends online and available for chatting.



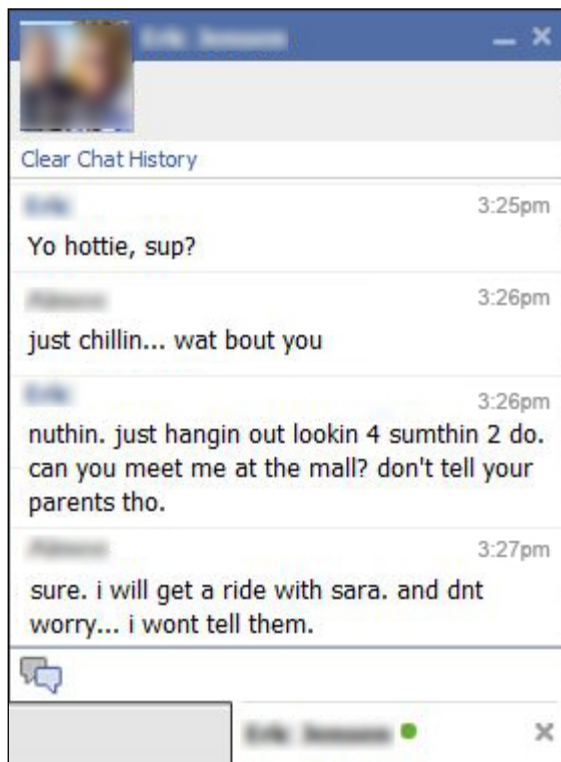
Facebook Chat

Several chat options can be accessed by clicking on the chat indicator:



Facebook Chat Setting

Chatting with friends is fun for teens, but as you can see, this could be very dangerous if the “friend” was a sexual predator:



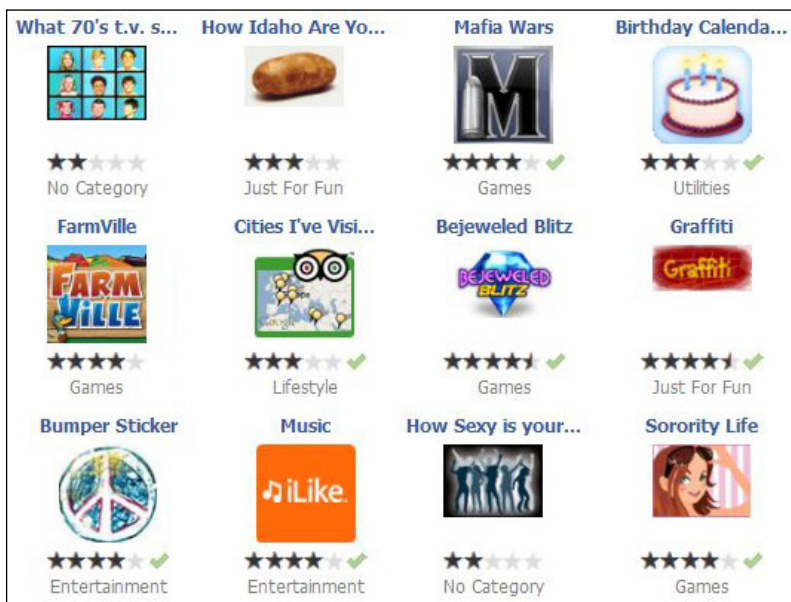
Facebook Chat Session

Applications

Some social networking websites allow members to subscribe to “applications” or “apps.” Applications are small programs that run within the website. There are thousands of applications that your teen can add to his or her webpage. Applications are a form of entertainment. They allow teens to play games, share social calendars, challenge others to trivia, and share links, just to name a few.

Some of the more popular applications are designed as surveys. They can collect detailed personal information such as hair color, weight, eye color, piercings, tattoos, drinking and smoking preferences, and education goals. That information is shared with other members listed as that individual's friends.

However, some applications collect or “mine” data, and share more information than your child may think. Once your teen has authorized the application, it can access all personal information, including contact information, videos, and photos. If the proper profile security settings are not in place, your teen's personal information could be disseminated to people that he or she does not know, and even used in web advertisements. Applications can also contain viruses and malicious spyware that can infect your computer. Your teen needs to be very careful when authorizing applications. Below is an example of some popular apps:



Applications in Facebook

Blogs

“Blog” is short for “weblog,” which is an online journal or diary. Members of social networking websites post blogs about a variety of topics, such as their personal interests, opinions, or simply their daily life. Teens may also use blogs to talk about the places they visit, share poetry they have written, or post lyrics to songs they like.

However, they need to be very cautious about the information they may leave on a blog. It is very easy to give away personal or location details that could lead a predator right to them.

The following example shows just how easy it can be for teens to let their emotions take over common sense when they are writing a blog.

Date: Jan 4, 2010

Finally!!!!!!!!!!!!!!

Current mood: 😊 fabulous

 So today was totally amazing! He finally asked me out! My parents hate him, but whatever. He wants me to meet him at the downtown Edwards Theaters this Friday night at 9:30 2 go c a movie. My parents will nvr let me do that with him! I will just tell them I am going with Dawn and Kate. I will have my mom drop me off at 8:30, then I'll chill at Starbucks by myself til Nate gets there. I LIKE HIM SO MUCH! <3 I am soooooo happpppeeeeeee. 😊

1:01 AM - 0 Kudos - 0 Comments - Add Comment - Edit - Delete

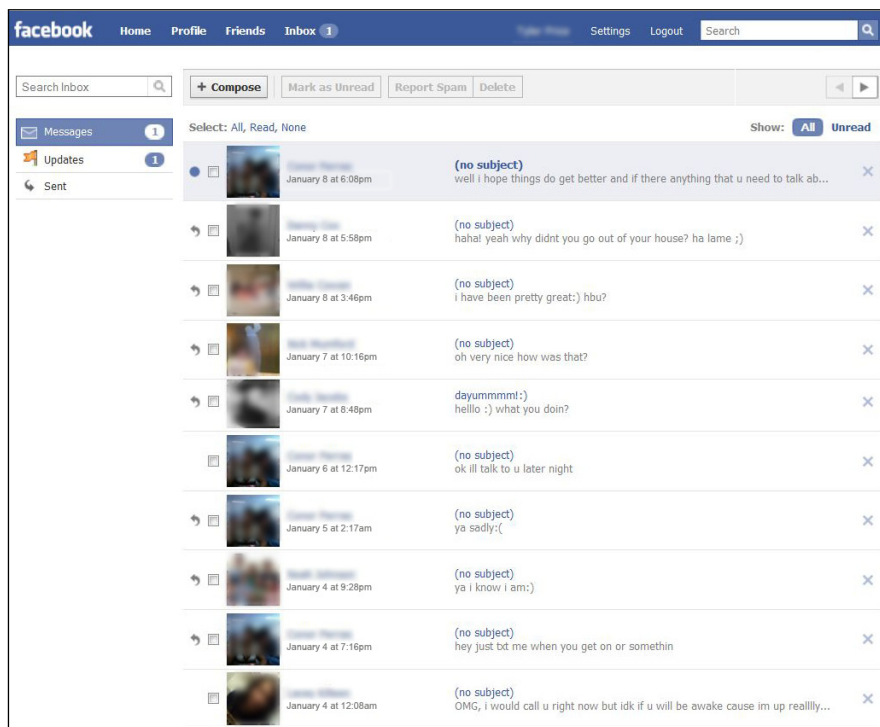
MySpace Blog

This blog provides a date and time when this teen will be alone at a downtown coffee shop. That information is all an Internet predator needs to have access to your child.

Mail Messages

Social networking websites all contain a form of private communication. Messages that are sent and received within the mail center are person-to-person, exactly like e-mail.

Many young people are using only the mail services within their social networking sites instead of accessing their Yahoo, Hotmail, and Gmail accounts. The following is an example of what mail messaging looks like in Facebook.



Facebook Mail Messages

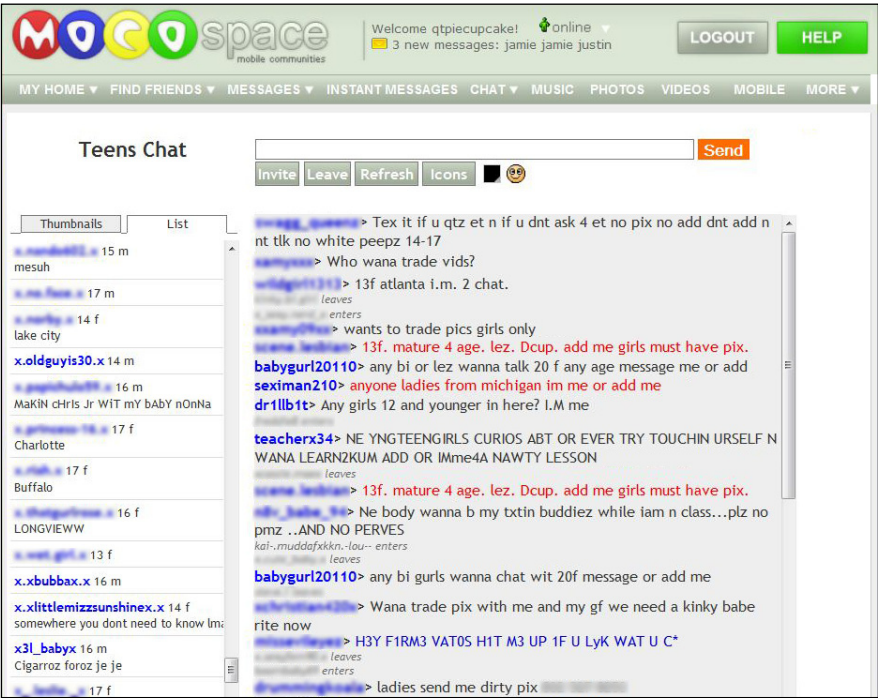
Chat Rooms

A chat room is a real-time public conversation room. These rooms are often frequented by people looking for sex. Conversations in these rooms can be very sexual in nature and even violent.

The two most popular social networking sites have removed the “chat room” function as a general option. However, a teen can add certain applications for the purposes of chat

rooms. Some social networking websites, such as MocoSpace, still allow members to join chat rooms as part of their standard profile.

The following example is quite disturbing. It shows a public chat room in MocoSpace. The room is titled “Teens Chat,” but as you can see, a significant amount of the conversations are not appropriate for a teen.



MocoSpace Teens Chat Room

Even more disturbing is the number of people in this chat room that are lying about their age. In several instances, the people were much older than what is listed on the left. For example, “x.oldguysis30.x” is listed as being a 14-year-old male. His profile age of 14 allows him to access this chat room. However, in the “About Me” section of his profile, he

states, “I am 30 years old not 14.” Encourage your teen to stay out of chat rooms altogether.

WHAT I CAN DO TO KEEP MY CHILD SAFE

The single most important thing you can do is understand and be involved in your children’s Internet activity. Sit down with them and review any profiles they have created or visited. Talk to them about their online safety, and teach them how they can be responsible on social networking sites.

Do your own research. Social networking websites have links to safety tips covering subjects such as inappropriate content, misrepresentations of age, and harassment. The following are some general safety tips that can be shared with teens who network online:

- Do not post information that enables a stranger to locate you. This includes personally identifying information such as: first name; last name; the name of your school or sports teams; the town you live in; or where you hang out.
- Create screen names that do not include real names, age, or gender.
- Never agree to meet in person someone whom you met online.
- Never post, send, or forward naked or sexually suggestive photos. Let them know that sending or keeping pictures of anyone under the age of 18 can be prosecuted as child pornography and that they could go to jail.
- Be careful about the photos you upload to your profile; do not post sexually suggestive images. Also, think about how the photos you post could affect your reputation if viewed by a college admissions counselor or potential employer.

- Do not reply to harassing messages. Tell a parent about any harassing or bullying situation.
- Do not reveal your password to others (except your parents). Doing so puts you at risk of being impersonated.
- Encourage your kids to talk to you or another adult if they come across information that upsets them, confuses them, or is pornographic.
- Make sure your child understands that not everything they read or see online is real, and that not all people are who they say they are.

Parents of teens who maintain profiles on social networking websites may want to monitor their children's online activities. Monitoring can include the following:

- Keep online computers in common areas of the home. Never put online computers in a child's bedroom.
- Keep a current record of your child's login information, including all e-mail addresses, login names, display names, and passwords.
- Regularly check your child's network of friends on each website. If there are people on the list that you do not know, ask your child who they are and how he or she met them. Remove "online only" friends on your child's profile. Remember, people aren't always who they say they are.
- Frequently check the content of your child's profile. Is your child posting inappropriate personal information, photos, videos, blogs, or comments? Is your child engaging in harassing or other inappropriate conduct? If so, remove the content.
- Verify that the security options on your child's accounts are appropriately set.

- Agree with your child upon a set of rules for using the Internet. A sample Family Contract for Internet Safety is provided at the end of this guide and on the ProtecTeens DVD.

If your child is exposed to inappropriate sexual material on a social networking website, there are several things you can do. Report sexually explicit material, child enticement, or unsolicited obscene material to local law enforcement and the CyberTipline at the National Center for Missing and Exploited Children, www.cybertipline.com, or (800) 843-5678. To learn more, visit www.missingkids.com.

On most social networking websites, you can also report inappropriate activity directly to the website. If you see inappropriate content or pictures, look for the “Report” link located on that webpage. If you cannot find one, copy the link from your browser address bar and send it to the company via its contact page.

UNDERSTAND CYBERBULLYING

According to the National Crime Prevention Council, almost half of all American teens have been the victim of cyberbullying. Cyberbullying happens when teens use the Internet, cell phones, or other digital devices to send or post messages or images that are intended to hurt, humiliate, or embarrass another person.

Forms of Cyberbullying

There are many different types of cyberbullying. Here are just a few examples:

- Sending or forwarding mean, threatening, discriminating, humiliating, embarrassing, or vindictive text messages, e-mails, or chats;

- Teasing or frightening someone online;
- Using lewd or insulting language and remarks;
- Using someone else's password to gain access to their account;
- Impersonating someone online;
- Spreading rumors or lies about someone through messages, comments, bulletins, or wall posts;
- Pretending to be someone you are not to gather information from others;
- Posting pictures or information about someone without their consent;
- Insulting someone while playing an interactive online game;
- Voting on an online bashing poll or guestbook.

Talk to your children about cyberbullying, and how it could affect them, both as a victim or as a participant. Make sure your teens understand that they should treat others with respect when they are texting or are online, and that there are stiff legal consequences for cyberbullying in Idaho.

Victims of Cyberbullying

The single most important thing you can do is let your teen know that they can come to you if they feel they have been the victim of a cyberbully. You can help your teen stay safe by having them follow these steps:

- Never forward or respond to mean, embarrassing, or hurtful messages or images to other people;
- Never share their passwords or other account information with anyone;
- Block any and all communications from a cyberbully;
- Never give personal information out to anyone;

- Immediately report cyberbully encounters to your school resource officer.

There are laws in Idaho that protect victims of harassment, intimidation, and bullying. If you feel that your child is the target of cyberbullying, talk to your school counselor or resource officer immediately. Cyberbullying can have very serious effects on your child.

DELETING A PROFILE

If you decide to delete your teen's profile, try to gain his or her cooperation first. Talk to your child about your concerns for his or her safety and other options for socializing with friends. Otherwise, your teen may go "underground" and set up another profile that is harder to trace or is on another social networking website.

Deleting or deactivating a profile often requires several steps. Individual social networking websites provide instructions on how to delete or deactivate accounts. It is important to carefully follow each step required, or the profile will not be deleted.

After you follow the deletion or deactivation steps, always check to make sure the profile is actually deleted.

For more information on teen Internet safety, visit www.ag.idaho.gov and view the ProtecTeens video. Additional information can be found on the Idaho Internet Crimes Against Children Task Force website at www.icacidaho.org.



ProtectTeens™

OFFICE OF ATTORNEY GENERAL
LAWRENCE WASDEN

FAMILY CONTRACT FOR INTERNET SAFETY

Child's Agreement

I know that there are strangers and dangers on the Internet. To help keep me safe, I promise to follow these steps whenever I am online.

- I will create safe and polite screen and profile names that do not tell people anything about me or my family, and are not rude or sexually suggestive.
- I will not give out or put any personal information about me or my family anytime I am online, including my address, telephone number, what school I go to, or how old I am.
- I will not add people as "friends" to my profile that I do not know personally and in real life.
- I will not be a cyberbully. I will treat others with respect, use good language, and not post or send anyone mean or threatening words that might hurt or embarrass them.
- I will not send pictures or videos of myself to anyone without asking my parents first.
- I will tell my parents about people I meet online. I know there are adults that will pretend to be kids to get me to talk to them.
- I will not call or agree to meet anyone I met online without asking my parents first.
- I will tell my parents immediately if someone sends or posts any pictures, videos, or words that make me uncomfortable, sad or upset.
- I will keep my screen names, profiles names and passwords secret from everyone except my parents.
- I will tell my parents if someone online asks me to do something I am not supposed to do or that makes me uncomfortable or embarrassed.
- I will not download anything from the Internet unless first asking my parents.
- I know that it is illegal to send or post sexually suggestive photos or videos of myself or friends.
- I will not buy or order anything online without asking my parents' permission first.
- I will follow my parents' guidelines for my Internet use anytime I am connected, whether I am at home, at school, or at a friend's house.

Parent Agreement

I know that the Internet can be a dangerous place, but that it can also be very useful and entertaining. I will help my child stay safe online by following these guidelines.

- I will be involved in my child's Internet activity, and get to know the websites they visit.
- I will set reasonable rules for my child's Internet use.
- I will listen to my child. If they have made an error in judgment using the Internet, I will react reasonably.
- I will keep a list of my child's profile names, e-mail addresses, and passwords.
- I will take steps to keep my family safe from strangers and inappropriate material on our computers.
- I will report any suspicious, inappropriate, or illegal activity to the proper authorities.
- I will frequently check to see what sites my child is visiting on the Internet.
- I will continue to learn about new ways to protect my family when they are online.

Child's Signature

Date

Parent's Signature

Date

Consumer Protection Manuals

Buying a Home	Landlord and Tenant Guidelines
Charitable Giving	A Parents' Guide to Social Networking Websites
Credit and Debt	Pyramids, Gift Schemes & Network Marketing
Foreclosure Prevention and Foreclosure Scams: How to Tell the Difference	Residential Construction
Guidelines for Motor Vehicle Advertising in Idaho	Rules of Consumer Protection
Idaho Consumer Protection Manual	Rules of Telephone Solicitations
Idaho Lemon Law	Senior Citizens Manual
Identity Theft	Service on an Idaho Nonprofit Board of Directors
Internet Lingo Dictionary	Telephone Solicitation
Internet Safety	Young Adult Handbook

This publication was prepared by the Attorney General's Consumer Protection Division and the Idaho Internet Crimes Against Children Task Force (Idaho ICAC).

Funds collected by the Attorney General's Consumer Protection Division as the result of enforcement actions paid for this pamphlet. No tax monies were used to pay for this publication.

The Consumer Protection Division enforces Idaho's consumer protection laws, provides information to the public on consumer issues, and offers an informal mediation process for individual consumer complaints.

If you have a consumer problem or question, please call (208) 334-2424 or in-state toll-free (800) 432-3545. TDD access and Language Line translation services are available. The Attorney General's website is available at www.ag.idaho.gov.

If you have information about an Internet crime against a child or that you think will be useful in the fight against child exploitation, contact us through the National CyberTipline at www.cybertipline.com or by calling, toll-free (800) 843-5678.

The information you provide will be forwarded to the appropriate ICAC law enforcement agencies in Idaho or elsewhere in the United States.